arXiv:1304.3893v2 [math.GR] 6 May 2013

Remarks on profinite groups having few open subgroups

Dan Segal

May 7, 2013

Let G be profinite group. If G is finitely generated, then every subgroup of finite index is open, the derived group G' is closed, and every power subgroup G^m is open. These results were established in [NS1] and [NS2] (for better proofs see also [NS3]). Might they be generalized to the case where G is not finitely generated, but is assumed to have only finitely many open subgroups of each finite index? In the context of Galois theory, this condition arises more naturally than finite generation.

The answer, unfortunately (?), is 'no'. [N], Section 6, gives examples of profinite groups G, having only finitely many open subgroups of each finite index, such that $G^2 < \overline{G^2} = G$; thus G has subgroups of index 2, none of which can be open ($\overline{X}$ denotes the closure of a subset X). Here we indicate a slightly simpler construction that yields:

Theorem 1 *Let S be a non-empty set of primes. There is a profinite group G with the following properties:*

(1) G is topologically perfect, i.e. $G = \overline{G'}$;

(2) $\overline{G^m}$ is open in G for each $m \in \mathbb{N}$; for each $k \in \mathbb{N}$, G has finitely many open subgroups of index k;

(3) if $m \in \mathbb{N}$ is coprime to S then G^m is open, and G has finitely many normal subgroups of index m;

(4) if $p \in S$ then $G/G'G^p$ is infinite, and G has uncountably many normal subgroups of index p, none of which is open;

(5) G' is not closed, and G^p is not closed for each $p \in S$.

In a positive direction, we have

Theorem 2 *Let G be a profinite group having only finitely many open subgroups of each finite index, and let $m \in \mathbb{N}$. Then $\overline{G^m}$ is open in G.*

It follows that if G^m is closed for every m, then every subgroup of finite index is indeed open in G (such a group is said to be *strongly complete*). Is the converse true? I expect not, but a counterexample does not seem easy to find. However, it is not hard to establish

Proposition 1 *There is a strongly complete profinite group Q in which Q' is not closed.*

Profinite groups having only finitely many open subgroups of each finite index arise in number theory: this property is enjoyed by the Galois group of the maximal algebraic extension field of $\mathbb{Q}$ unramified outside a given finite set of primes ([K], Theorem 1.48). With Chebotarev's Theorem ([K], Theorem 1.116), Theorem 2 becomes in this context

Corollary 1 *Let S be a finite set of primes and let $m \in \mathbb{N}$. Then there are only finitely many finite Galois extensions K of $\mathbb{Q}$ such that* (1) *all primes ramified in K are in S and* (2) *almost all primes have residue degree at most m in K.*

Remark. If we assume that G has only finitely many *abstract* subgroups of each finite index, then these are indeed all open. In fact it is shown in [SW2] that for a profinite group, the following three conditions are equivalent:

- every finite-index subgroup is open,
- for each n there are only finitely many subgroups of index n,
- for each n there are only countably many subgroups of index n.

I will use the following notation. For subset X of a group,

$$X^{*n} = \{x_1 x_2 \dots x_n \mid x_1, x_2, \dots, x_n \in X\}.$$

For a group word w on k variables,

$$G_w = \{w(\mathbf{g})^{\pm 1} \mid \mathbf{g} \in G^{(k)}\}, \quad w(G) = \langle G_w \rangle\,;$$

and for $m \in \mathbb{N}$, $G_{\{m\}} = \{g^m \mid g \in G\}$, $G^m = \left\langle G_{\{m\}} \right\rangle$.

The word w has width f in G if $w(G) = G_w^{*f}$, and infinite width if this holds for no finite f. We recall that in a profinite group G, the subgroup $w(G)$ is closed if and only if w has finite width in G; this holds if and only if w has bounded width in all the finite quotients G/N with N open and normal in G (see [S], Section 4.1).

We need a slight generalization:

Lemma 1 *Let G be a profinite group and w a word. If $w(G)$ has finite index in its closure $\overline{w(G)}$ then w has finite width in G, and so $w(G) = \overline{w(G)}$.*

Proof. Put $H = \overline{w(G)}$. Then $H = w(G)T$ for some finite set T, so

$$H = \bigcup_{n=1}^{\infty} X_n T$$

where $X_n = G_w^{*n}$, an ascending union. Baire's Category Theorem now shows that $X_n T$ contains a non-empty open subset U of H, for some n. In turn

$U \supseteq Nh$ for some open normal subgroup N of H and some $h \in H$. It follows that $H = X_n Y$ for some finite set Y and then $w(G) = X_n(Y \cap w(G)) \subseteq X_n X_{n'} = X_{n+n'}$ for some n'. Thus w has width $n+n'$ in G. (A slight modification to the argument shows that in fact $\overline{w(G)}/w(G)$ must be either trivial or uncountable.) ■

The key to Theorem 1 is the following construction due to Derek Holt:

Lemma 2 ([H], Lemma 2.2) *Let $q > 3$ be a power of a prime p, and let $r \in \mathbb{N}$. Then there is a perfect finite group $K = K(q,r)$ such that $K = P \rtimes H$ where $H = \mathrm{SL}_2(\mathbb{F}_q)$, $P = [P,H]$, and $P \cap \mathrm{Z}(K)$ contains an elementary abelian subgroup N with $|P : N| = q^{2r}$ and $|N| = q^{r(r+1)/2}$.*

Since K is perfect we have $K = K'K^p = w(K)$ where $w(x,y,z) = [x,y]z^p$. Suppose that w has width f in K. Then $|K/N|^{3f} \geq |K|$. A crude estimate (using the fact that $|H| < q^3$) then yields $f > r/12$.

Now let $(q_n = p_n^{e_n})$ be a strictly increasing sequence of prime powers exceeding 3, such that every prime in S occurs infinitely often among the p_n, and every p_n is in S. I claim that the profinite group

$$G = \prod_{n=1}^{\infty} K(q_n, 12n)$$

satisfies (1) – (5) of Theorem 1.

(1) is clear. (2) We have

$$K_n := K(q_n, 12n) = P_n \rtimes H_n \text{ where } H_n = \mathrm{SL}_2(\mathbb{F}_{q_n}).$$

Given m, there exists s such that $H_n = H_n^m$ for all $n > s$, and then

$$K_n^m \geq H_n[P_n, H_n] = K_n.$$

So $\overline{G^m}$ contains $\prod_{n>s} K_n$ which is open in G.

Every open subgroup of index k contains $\overline{G^m}$ where $m = k!$, so the number of such subgroups is finite.

(3) If m is coprime to S then every element of P_n is an mth power, for each n. By [MZ], [SW], every element of H_n is a product of $k = k(m)$ mth powers provided $n > s$ (s as above; the result quoted refers to simple groups, but easily extends to $\mathrm{SL}_2(\mathbb{F}_q)$ since -1 is a square in this group). The set $G_{\{m\}}^{*(k+1)}$ is closed and contains K_n for each $n > s$; consequently

$$G^m \supseteq G_{\{m\}}^{*(k+1)} = \overline{G_{\{m\}}^{*(k+1)}} \supseteq \prod_{n>s} K_n,$$

so G^m is open. The second claim is then clear.

(4) The word $w = [x,y]z^p$ does not have width n in K_n whenever $p_n = p$; as this occurs for infinitely many values of n it follows that w has infinite width in G. Now Lemma 1 shows that $w(G) = G'G^p$ has infinite index in $\overline{w(G)} = G$. The final claim is then immediate (a group of order p can't be perfect!).

(5) Of course (1) and (4) imply that G' is not closed. If $p \in S$ and G^p is closed then G^p is contained in a open normal subgroup of index p, contradicting (4).

Proposition 1 is even simpler. For each prime p let M_p be a finite p-group such that the word $[x,y]$ does not have width p in M_p; easy examples are given in [S], Section 3.2. We take

$$Q = \prod_{p \text{ prime}} M_p.$$

Then $[x,y]$ has infinite width in Q, so Q' is not closed. Now let $m \in \mathbb{N}$. Then $M_p = (M_p)_{\{m\}}$ for every prime p not dividing m. It follows that

$$Q^m \supseteq Q_{\{m\}} = \overline{Q_{\{m\}}} \supseteq \prod_{p>m} M_p,$$

so Q^m is open. Every subgroup of index k in Q contains Q^m where $m = k!$, so the number of such subgroups is finite.

Now we turn to Theorem 2. This is a generalization of the positive solution to the restricted Burnside problem, and the proof is essentially the same. Write $s_n(G)$ to denote the number of subgroups of index at most n in a finite group G. Then Theorem 2 will follow if we establish

Theorem 3 *Let $f : \mathbb{N} \to \mathbb{N}$ be a function and let $m \in \mathbb{N}$. If G is a finite group such that $G^m = 1$ and $s_n(G) \leq f(n)$ for all n then $|G| \leq \nu(m,f)$, a number depending only on f and m.*

From now on, all groups will be finite. Let us define the *height* of G to be the minimal length $h(G)$ of a chain of normal subgroups $1 = G_0 < G_1 < \ldots < G_n = G$ such that each factor G_i/G_{i-1} is either nilpotent or semisimple; a semisimple group is a direct product of non-abelian simple groups.

Theorem 4 (Hall and Higman) *If $G^m = 1$ then $h(G) \leq \eta(m)$, a number depending only on m.*

This follows from Theorem A and (the proof of) Theorem 4.4.1 in [HH], together with the fact (not yet proved in 1956) that $\mathrm{Out}(S)$ is soluble of derived length at most 3 whenever S is a non-abelian finite simple group (see [GLS], sections 7.1 and 2.5). An explicit function η is easily obtained by following through the Hall-Higman argument.

Now let G be a group satisfying the hypotheses of Theorem 3.

Case 1. Suppose that $|G| = p^e$ for some prime p, and that $|G/G'G^p| = p^d$. Then $p^{d-1} \leq s_p(G) \leq f(p)$ so $d \leq \delta(p) := \lceil 1 + \log_p f(p) \rceil$. Now G can be generated by d elements, and then Zelmanov's theorem [Z1], [Z2] gives $|G| \leq \beta(\delta(p), m)$, a number depending only on $f(p)$ and m.

Case 2. Suppose that G is nilpotent. Say $m = p_1^{e_1} \dots p_r^{e_r}$. Then from Case 1 we see that

$$|G| \leq \prod_{i=1}^{r} \beta(\delta(p_i), m) := \nu_{\mathrm{nil}}(m, f).$$

Case 3. Suppose that G is semisimple. The result of [J], with CFSG, shows that there are only finitely many non-abelian simple groups S such that $S^m = 1$; call them $S_1, \dots, S_k$ and put $t_i = |S_i|$. Now $G \cong \prod S_i^{(c_i)}$ for some $c_i \geq 0$. Clearly $c_i \leq s_{t_i}(G) \leq f(t_i)$ for each i, and so

$$|G| \leq \prod_{i=1}^{k} t_i^{f(t_i)} := \nu_{\mathrm{ss}}(m, f).$$

So far, we have shown that if $h(G) = 1$ then

$$|G| \leq \max\{\nu_{\mathrm{nil}}(m, f),\ \nu_{\mathrm{ss}}(m, f)\} := \nu_1(m, f),$$

say. Now let $q > 1$ and suppose inductively that for each $h < q$, and every function g, we have found a number $\nu_h(m, g)$ such that for any group H satisfying $h(H) \leq h$, $H^m = 1$ and $s_n(H) \leq g(n)$ for all n we have $|H| \leq \nu_h(m, g)$.

Define

$$\nu_q(m, f) = \nu_1(m, f) \cdot \nu_{q-1}(m, g_{m,f})$$

where $g_{m,f}(n) = f(n.\nu_1(m, f))$. Suppose that G with $G^m = 1$ satifies $s_n(G) \leq f(n)$ for all n and that $h(G) \leq q$. Thus G has a normal subgroup H with $h(H) \leq q - 1$ such that G/H is either nilpotent or semisimple. Then $|G/H| \leq \nu_1(m, f)$, and so for each n we have

$$s_n(H) \leq s_{n.\nu_1(m,f)}(G) \leq g_{m,f}(n).$$

Therefore $|H| \leq \nu_{q-1}(m, g_{m,f})$, whence $|G| = |H|\,|G/H| \leq \nu_q(m, f)$.

Finally, set

$$\nu(m, f) = \nu_{\eta(m)}(m, f).$$

If G satisfies the hypotheses of Theorem 3 then $h(G) \leq \eta(m)$ by Theorem 4 and so $|G| \leq \nu(m, f)$ as required.

References

[GLS] D. Gorenstein, R. Lyons and R. Solomon, *The classification of the finite simple groups, no.3*, American Math. Soc., Providence, Rhode Island, 1998.

[H] D. F. Holt, Enumerating perfect groups, *J. London Math. Soc. (2)* **39** (1989)**,** 67-78.

[HH] P. Hall and G. Higman, On the p-length of p-soluble groups and reduction theorems for Burnside's problem, Proc. London Math. Soc. (3) **6** (1956), 1-42.

[K] H. Koch, *Algebraic Number Theory,* Springer-Verlag, Berlin Heidelberg 1997.

[J] G. A. Jones, Varieties and simple groups, *J. Austral. Math. Soc.* **17** (1974), 163–173.

[MZ] C. Martinez and E. Zelmanov, Products of powers in finite simple groups. *Israel J. Math.* **96** (1996), 469-479.

[N] N. Nikolov, Algebraic properties of profinite groups, arXiv:1108.5130.

[NS1] N. Nikolov and D. Segal, On finitely generated profinite groups, I: strong completeness and uniform bounds, *Annals of Math.* **165** (2007), 171–238.

[NS2] N. Nikolov and D. Segal, Powers in finite groups, *Groups, Geometry and Dynamics* **5** (2011), 501-507.

[NS3] N. Nikolov and D. Segal, Generators and commutators in finite groups; abstract quotients of compact groups, *Invent. Math.* **190** (2012), 513-602.

[S] D. Segal, *Words: notes on verbal width in groups,* London Math. Soc. Lecture Notes Series **361**, Cambridge Univ. Press, Cambridge, 2009.

[SW] J. Saxl and J. S. Wilson, A note on powers in simple groups. *Math. Proc. Camb. Phil. Soc.* **122** (1997), 91-94.

[SW2] M. G. Smith and J. S. Wilson, On subgroups of finite index in compact Hausdorff groups, *Arch. Math.* **80** (2003), 123-129.

[Z1] E. I. Zelmanov, The solution of the restricted Burnside problem for groups of odd exponent, *Math. USSR Izv.* **36** (1991), 41–60.

[Z2] E. I. Zelmanov, The solution of the restricted Burnside problem for 2-groups, *Mat. Sb.* **182** (1991), 568–592.